Configurazione di ISE 2.0 e crittografia AnyConnect 4.2 Posture BitLocker Encryption

Sommario

Introduzione

In questo documento viene descritto come crittografare la partizione del disco dell'endpoint con Microsoft BitLocker e come configurare Cisco Identity Services Engine (ISE) per fornire l'accesso completo alla rete, solo quando è configurata la crittografia corretta. Cisco ISE versione 2.0 e AnyConnect Secure Mobility Client 4.2 supportano la postura per la crittografia del disco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione CLI di Adaptive Security Appliance (ASA) e configurazione VPN SSL (Secure Sockets Layer)
- Configurazione della VPN di accesso remoto sull'appliance ASA
- Servizi ISE e postura

Componenti usati

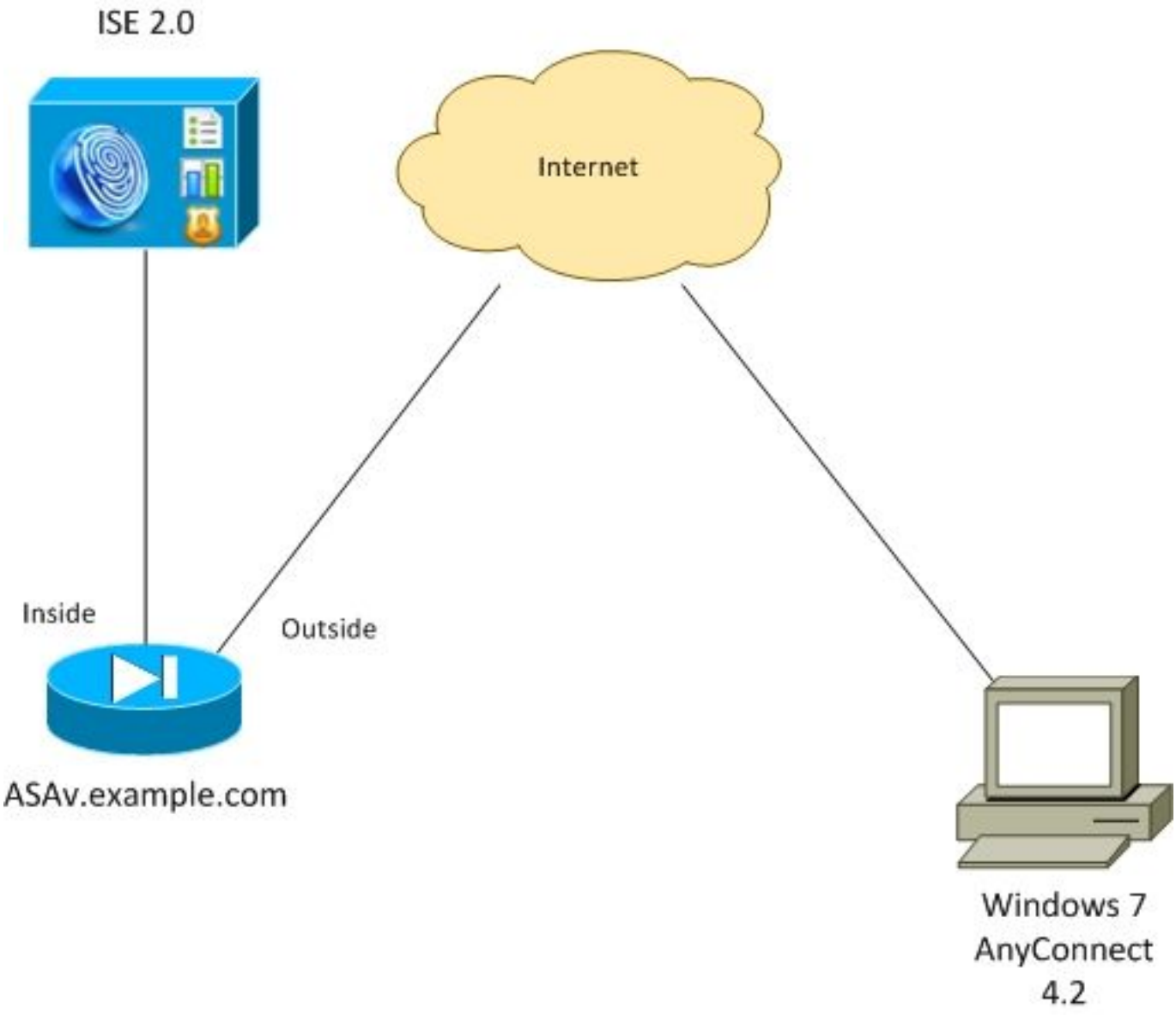
Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco ASA versione 9.2.1 e successive
- Microsoft Windows versione 7 con Cisco AnyConnect Secure Mobility Client versione 4.2 e successive
- Cisco ISE versione 2.0 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Il flusso è il seguente:

- La sessione VPN avviata dal client AnyConnect viene autenticata tramite ISE. Lo stato della postura dell'endpoint non è noto, la regola **ASA VPN** è **sconosciuta** e viene quindi reindirizzata all'ISE per il provisioning

- L'utente apre il browser Web, il traffico HTTP viene reindirizzato dall'ASA all'ISE. ISE invia all'endpoint la versione più recente di AnyConnect insieme al modulo di postura e conformità

- Una volta eseguito il modulo di postura, verifica se la partizione **E:** è completamente crittografato da BitLocker. In caso affermativo, il report viene inviato all'ISE che attiva la funzione Radius Change of Authorization (CoA) senza alcun ACL (accesso completo)

- La sessione VPN sull'appliance ASA viene aggiornata, l'ACL di reindirizzamento viene rimosso e la sessione ha accesso completo

La sessione VPN viene presentata come esempio. La funzionalità di postura funziona bene anche per altri tipi di accesso.

ASA

Èconfigurata dall'accesso VPN SSL remoto con l'uso di ISE come server di autenticazione, autorizzazione e accounting (AAA). È necessario configurare Radius CoA con ACL REDIRECT:

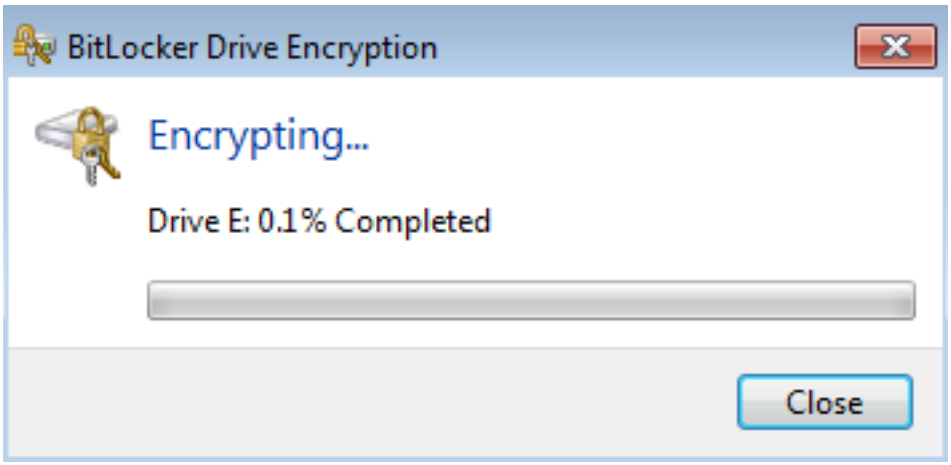
```
aaa-server ISE20 protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE20 (inside) host 10.48.17.235
 key cisco

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
 address-pool POOL
authentication-server-group ISE20
 accounting-server-group ISE20
 default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
 group-alias TAC enable

group-policy AllProtocols internal
group-policy AllProtocols attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable

access-list REDIRECT extended deny udp any any eq domain
access-list REDIRECT extended deny ip any host 10.48.17.235
access-list REDIRECT extended deny icmp any any
access-list REDIRECT extended permit tcp any any eq www

ip local pool POOL 172.16.31.10-172.16.31.20 mask 255.255.255.0
```

Per ulteriori informazioni, fare riferimento a:

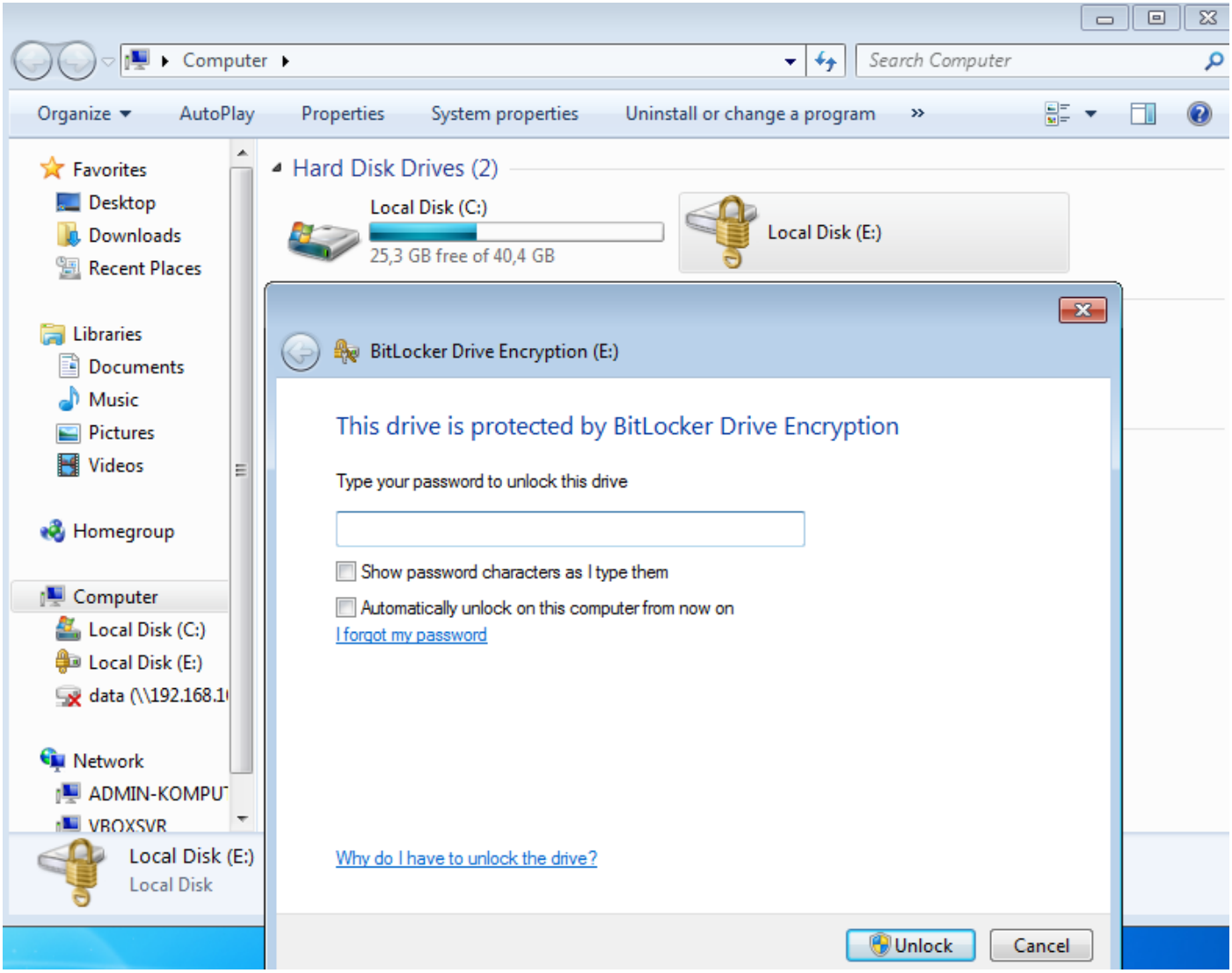
[Esempio di configurazione dell'integrazione di AnyConnect 4.0 con ISE versione 1.3]

BitLocker in Windows 7

Passare a **Pannello di controllo > Sistema e sicurezza > Crittografia unità BitLocker**, attivare **E:** crittografia della partizione. Proteggerlo con una password (PIN) come mostrato nell'immagine.



Una volta crittografata, installarla (fornendo la password) e verificare che sia accessibile, come mostrato nell'immagine.



Per ulteriori informazioni, consultare la documentazione Microsoft:

[Guida dettagliata a Crittografia unità BitLocker di Windows]

ISE

Passaggio 1. Dispositivo di rete

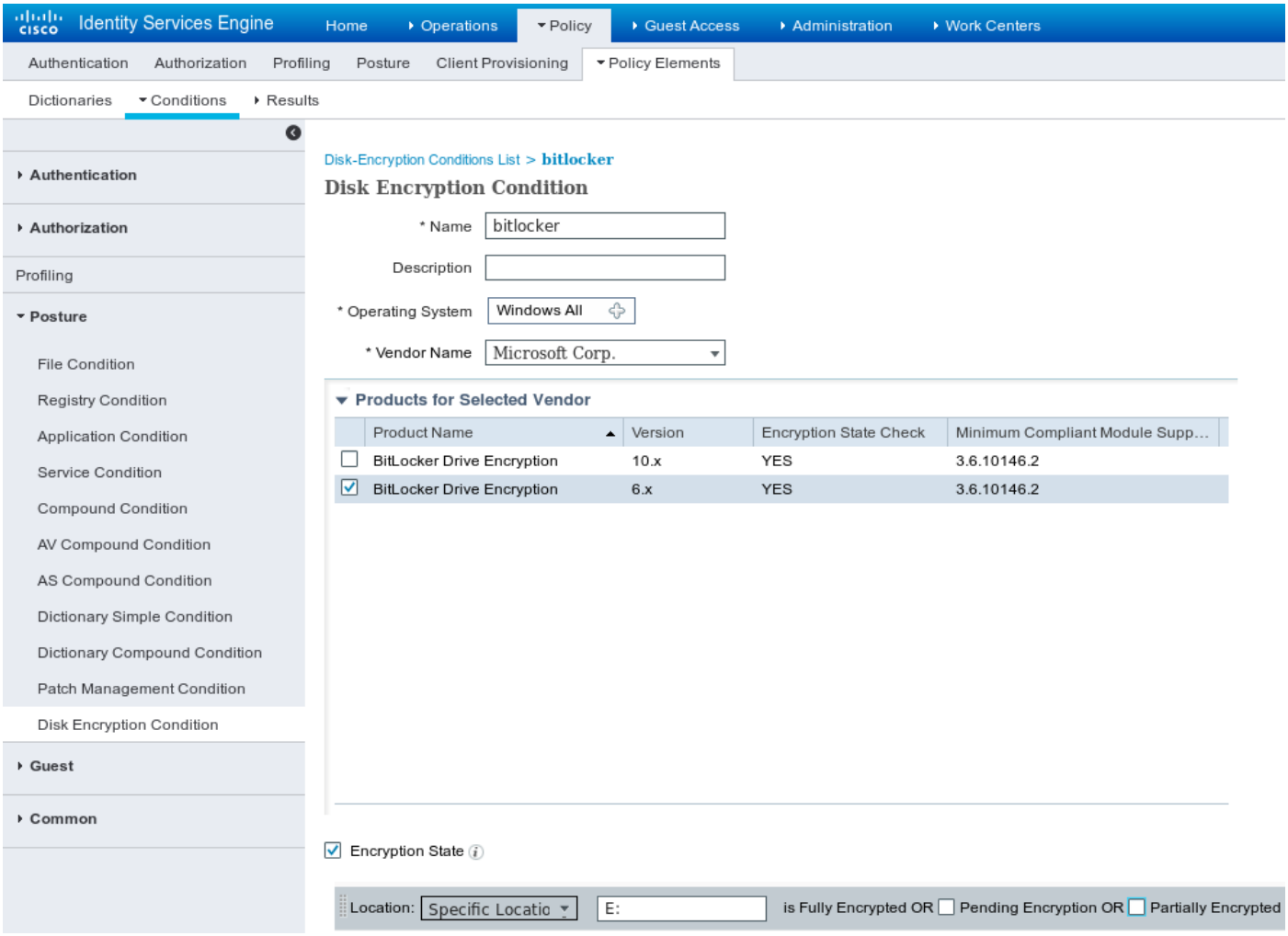
Selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**, Aggiungi **ASA con Tipo di dispositivo = ASA**. Viene utilizzata come condizione nelle regole di autorizzazione, ma non è obbligatoria (è possibile utilizzare altri tipi di condizioni).

Se appropriato, il gruppo di dispositivi di rete non esiste. Per creare, selezionare **Amministrazione > Risorse di rete > Gruppi di dispositivi di rete**.

Passaggio 2. Condizioni e criteri di postura

Assicurarsi che le condizioni di postura siano aggiornate: Selezionare **Amministrazione > Sistema > Impostazioni > Postura > Aggiornamenti > Aggiorna ora**.

Passare a **Criteri > Elementi criterio > Condizioni > Postura > Condizione crittografia disco**, quindi aggiungere una nuova condizione come mostrato nell'immagine.

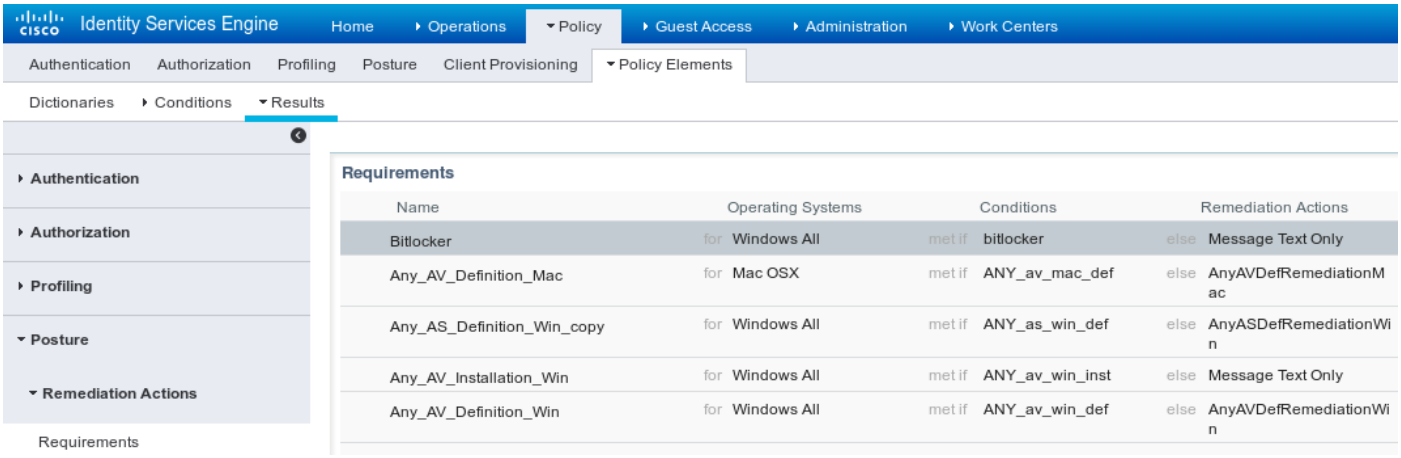


Questa condizione verifica se BitLocker per Windows 7 è installato e se **E:** la partizione è

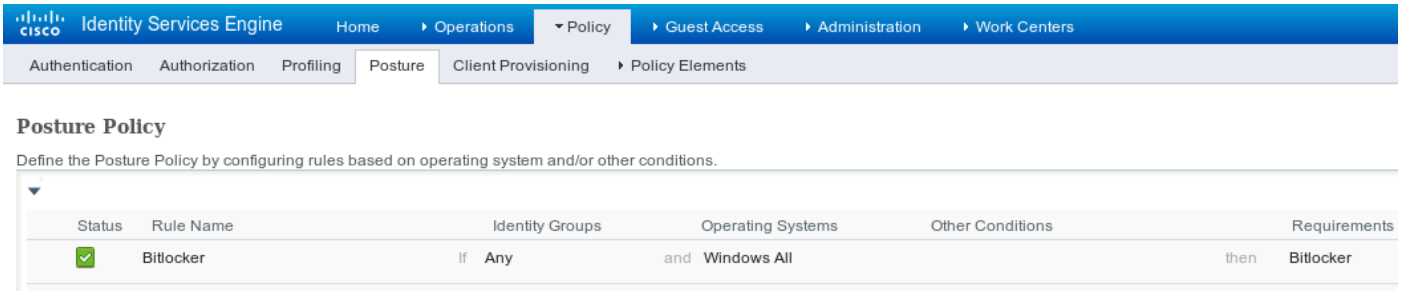
completamente crittografata.

> **Nota:** BitLocker è una crittografia a livello di disco e non supporta l'argomento Percorso specifico con solo lettera disco.

Passare a **Criterio > Elementi criteri > Risultati > Postura > Requisiti** per creare un nuovo requisito che utilizza la condizione come mostrato nell'immagine.

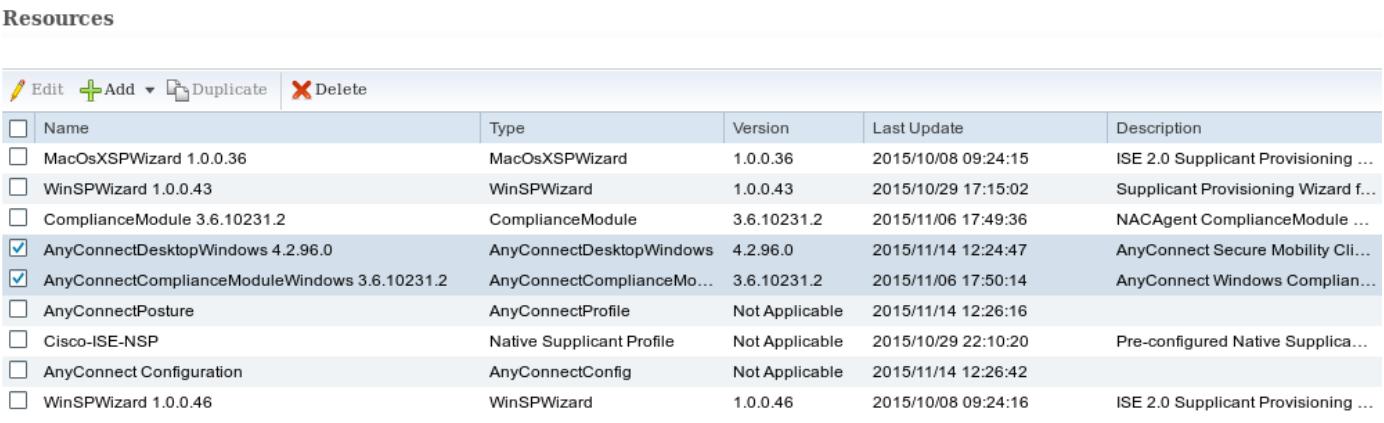


Passare a **Criterio > Postura**, aggiungere una condizione per tutte le finestre in modo da utilizzare il requisito come mostrato nell'immagine.



Passaggio 3. Risorse e criteri di provisioning client

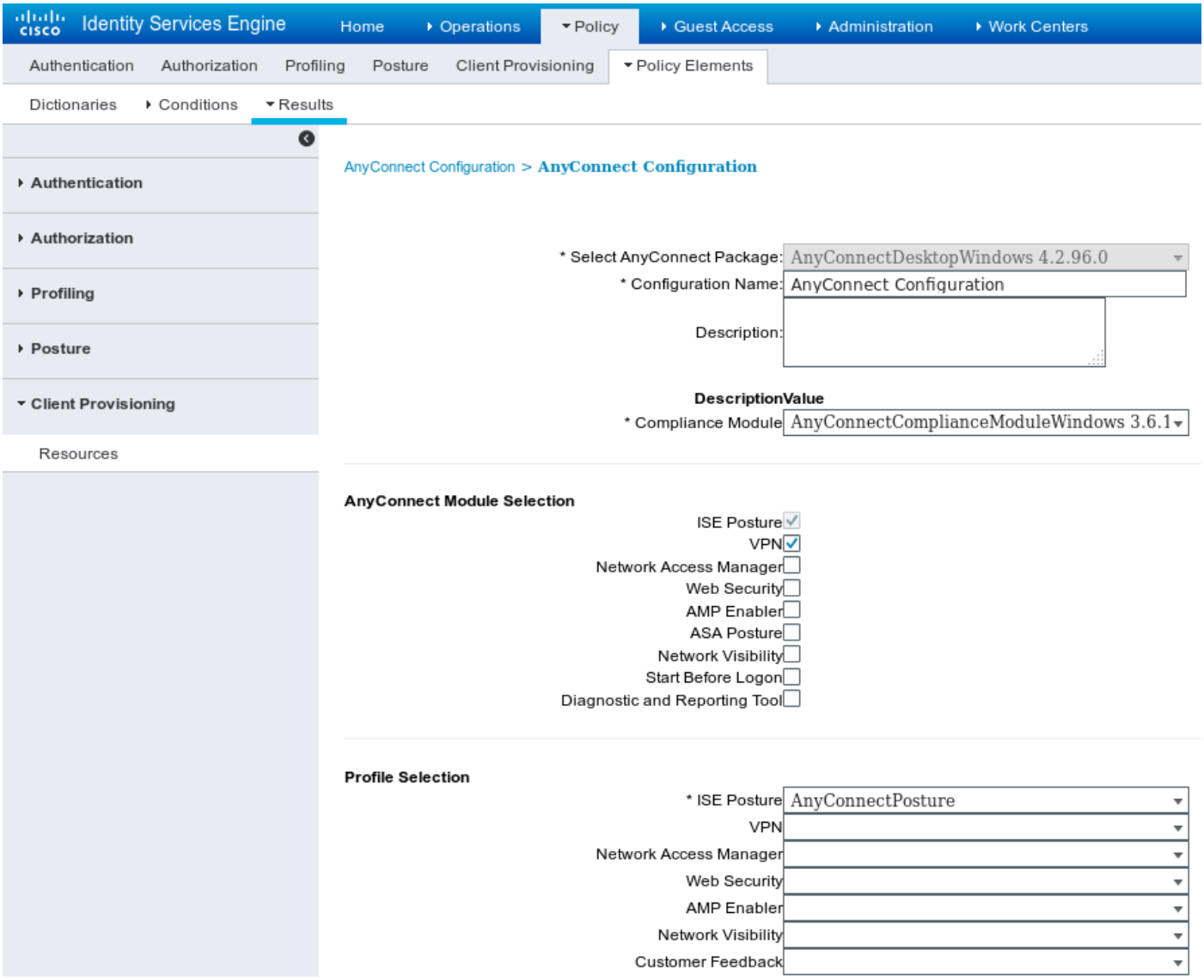
Selezionare **Policy > Policy Elements > Client Provisioning > Resources**, scaricare **Compliance Module** da Cisco.com e caricare manualmente il **pacchetto AnyConnect 4.2**, come mostrato nell'immagine.



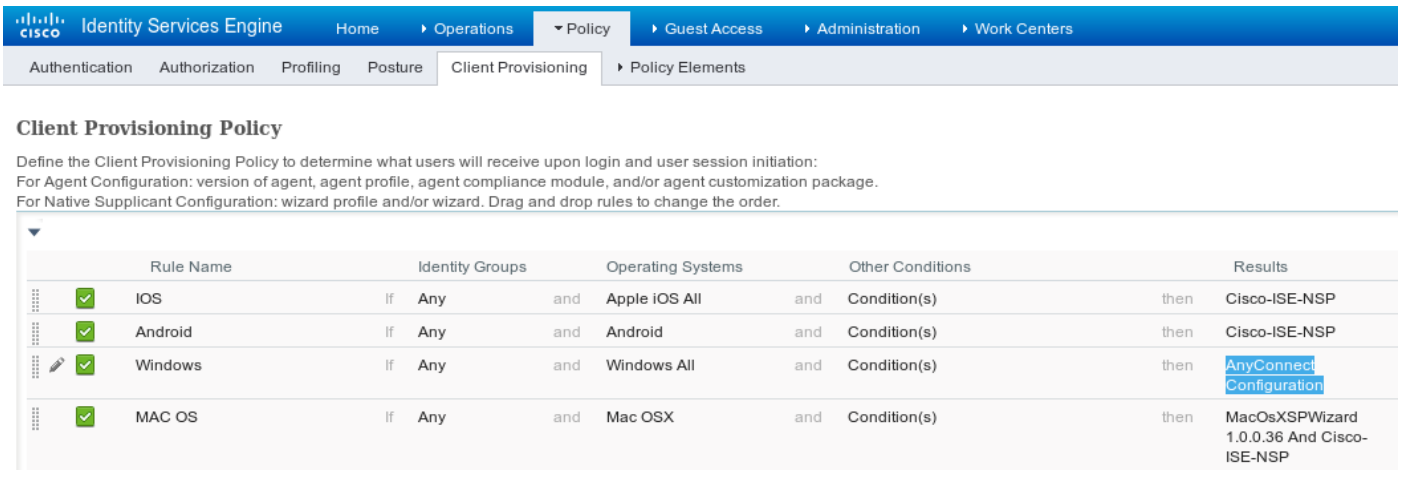
Selezionare **Add > NAC Agent o AnyConnect Posture Profile**, quindi creare il profilo AnyConnect

Posture (nome: **AnyConnectPosture**) con impostazioni predefinite.

Selezionare **Add > AnyConnect Configuration**, add AnyConnect profile (nome: **AnyConnect Configuration**) come mostrato nell'immagine.

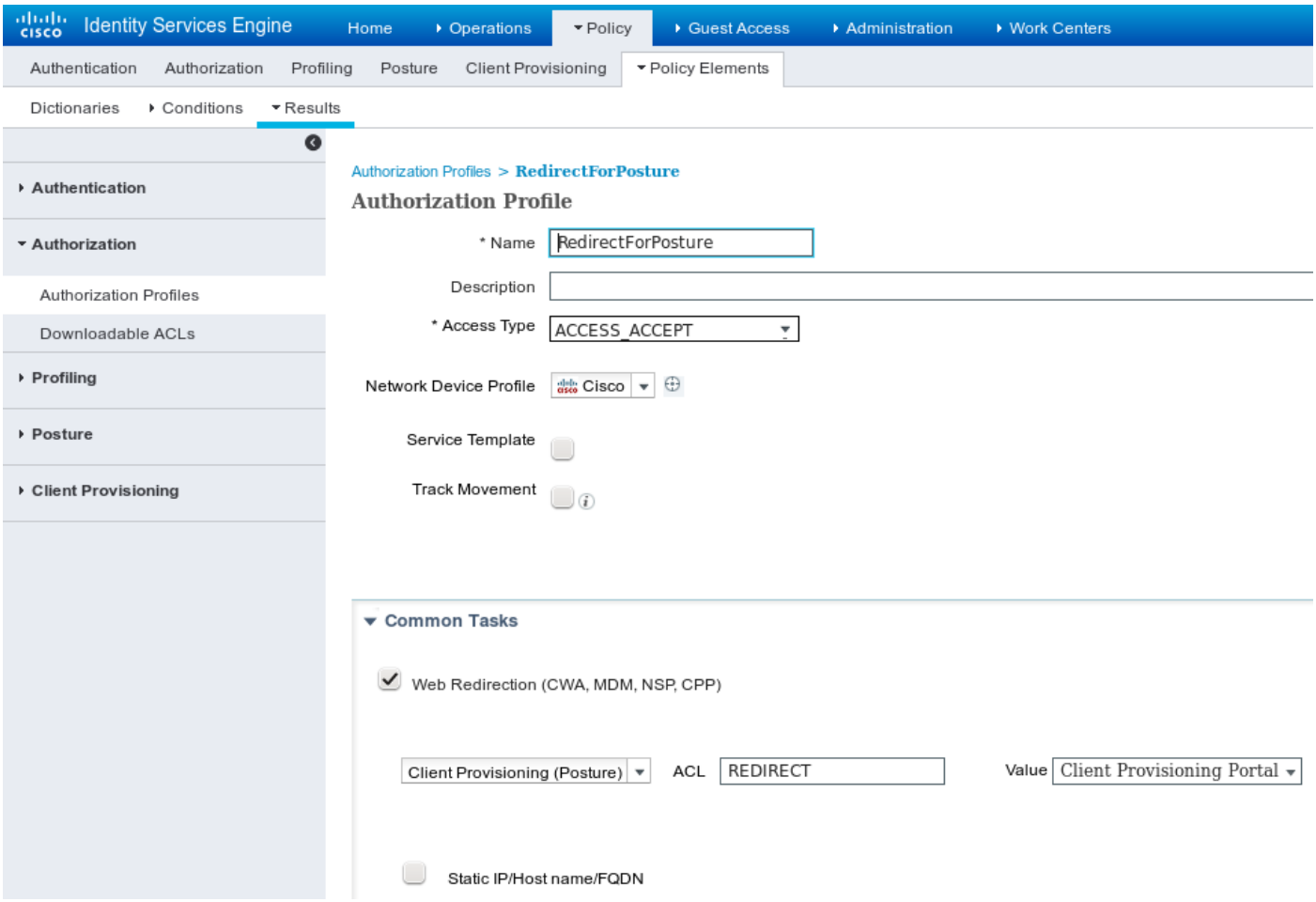


Selezionare **Policy > Client Provisioning** e modificare i criteri predefiniti per Windows in modo da usare il profilo AnyConnect configurato, come mostrato nell'immagine.



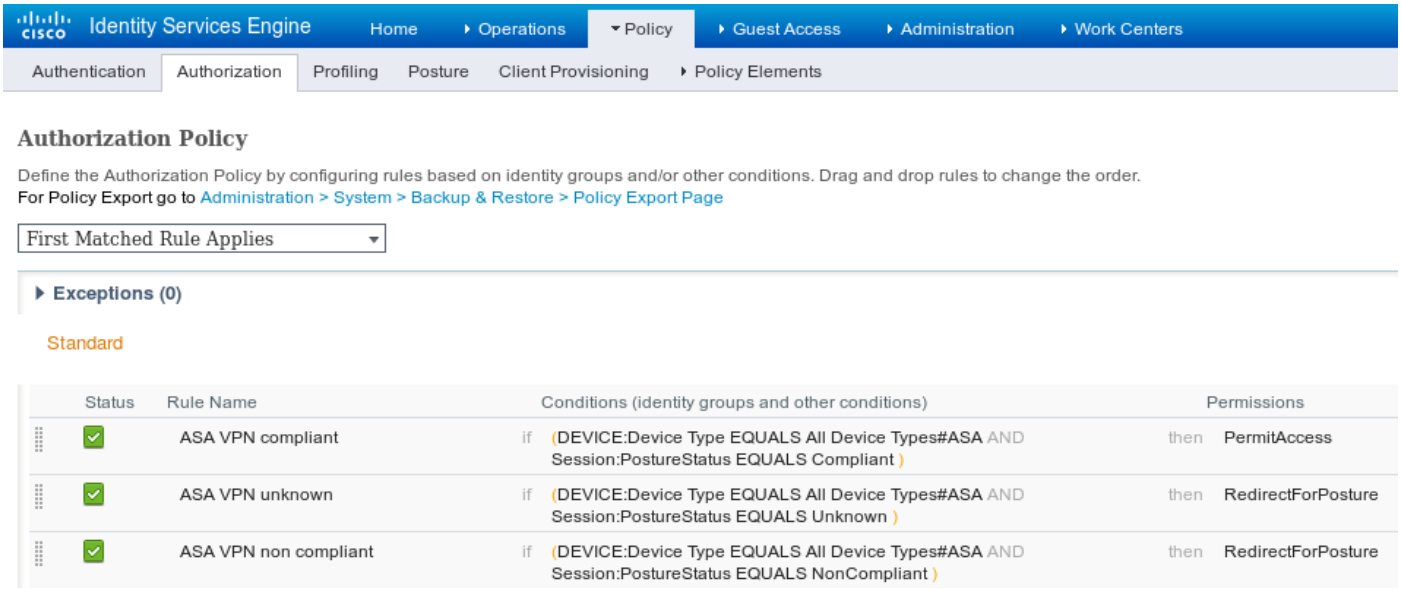
Passaggio 4. Regole di autorizzazione

Passare a **Criterio > Elementi criterio > Risultati > Autorizzazione**, aggiungere il profilo di autorizzazione (nome: **RedirectForPosture**) che reindirizza a un portale di provisioning client predefinito, come mostrato nell'immagine.



L'ACL **REDIRECT** è definito sull'appliance ASA.

Passare a **Criterio > Autorizzazione**, creare 3 regole di autorizzazione come mostrato nell'immagine.



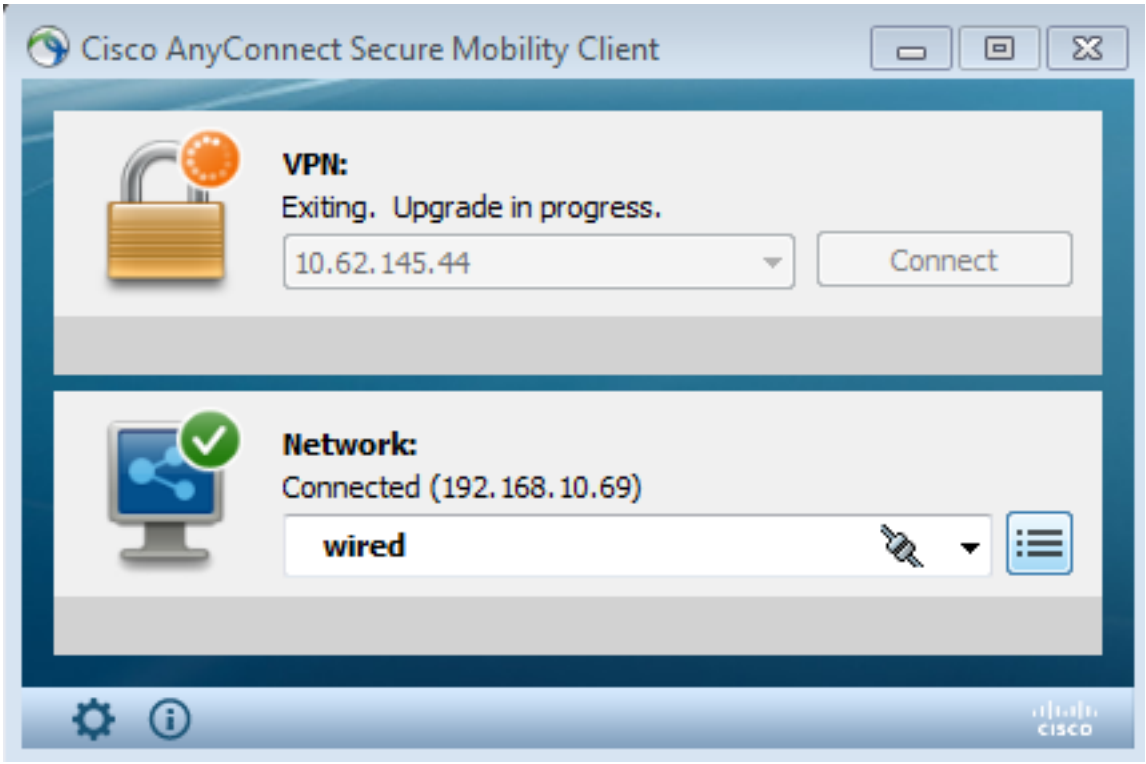
Se l'endpoint è conforme, viene fornito l'accesso completo. Se lo stato è sconosciuto o non conforme, viene restituito il reindirizzamento per il provisioning client.

Verifica

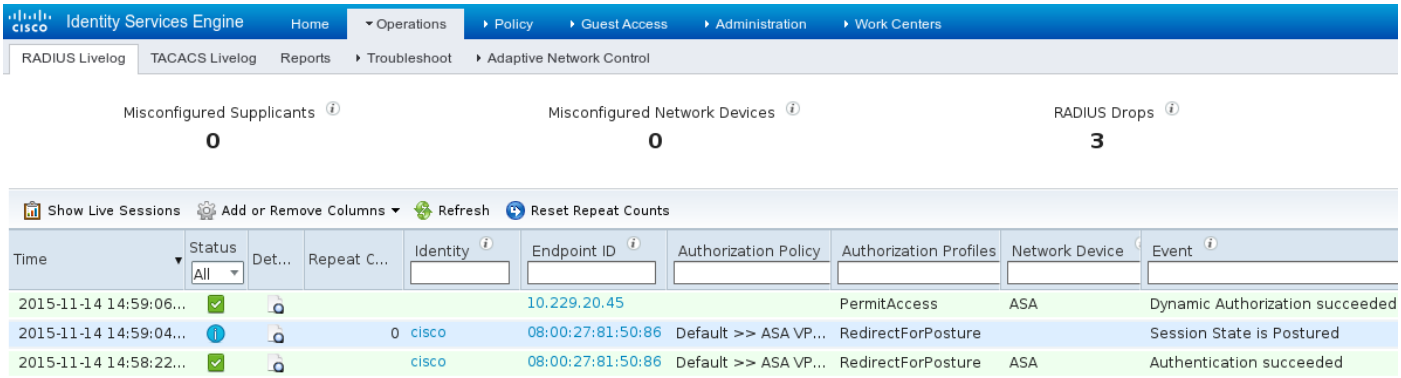
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passaggio 1. Definizione della sessione VPN

Una volta stabilita la sessione VPN, ASA potrebbe voler eseguire un aggiornamento dei moduli AnyConnect, come mostrato nell'immagine.



Su ISE viene trovata l'ultima regola, di conseguenza le autorizzazioni **RedirectForPosture** vengono restituite come mostrato nell'immagine.



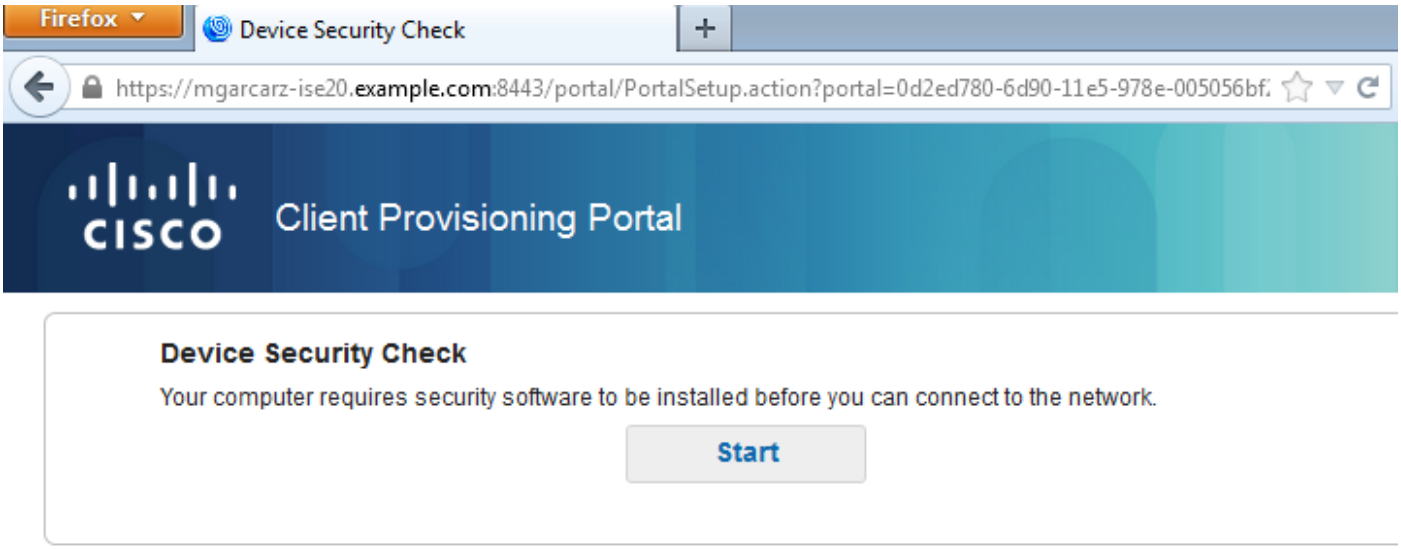
Una volta completata la creazione della sessione VPN, l'ASA segnala che il reindirizzamento deve essere eseguito:

```
ASAv# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 32
```

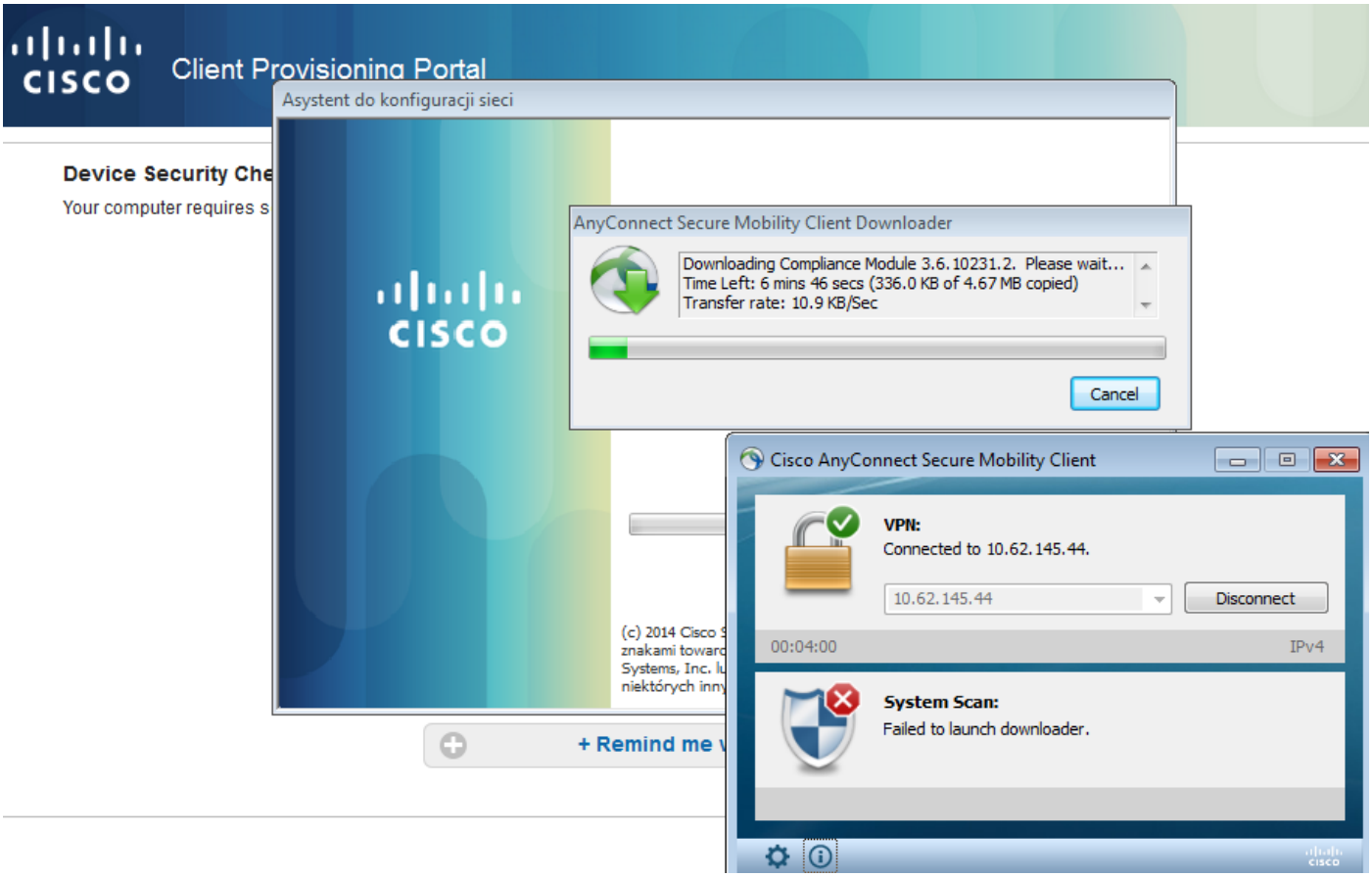
```
Assigned IP  : 172.16.31.10           Public IP    : 10.61.90.226
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 53201                 Bytes Rx     : 122712
Pkts Tx      : 134                   Pkts Rx      : 557
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : AllProtocols          Tunnel Group : TAC
Login Time   : 21:29:50 UTC Sat Nov 14 2015
Duration     : 0h:56m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a801010002000056647a7ce
Security Grp : none

<some output omitted for clarity>

ISE Posture:
  Redirect URL : https://mgarcarz-
ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-00505...
  Redirect ACL : REDIRECT
```

Passaggio 2. Provisioning client

In questa fase, il traffico del browser Web dell'endpoint viene reindirizzato ad ISE per il provisioning del client, come mostrato nell'immagine.

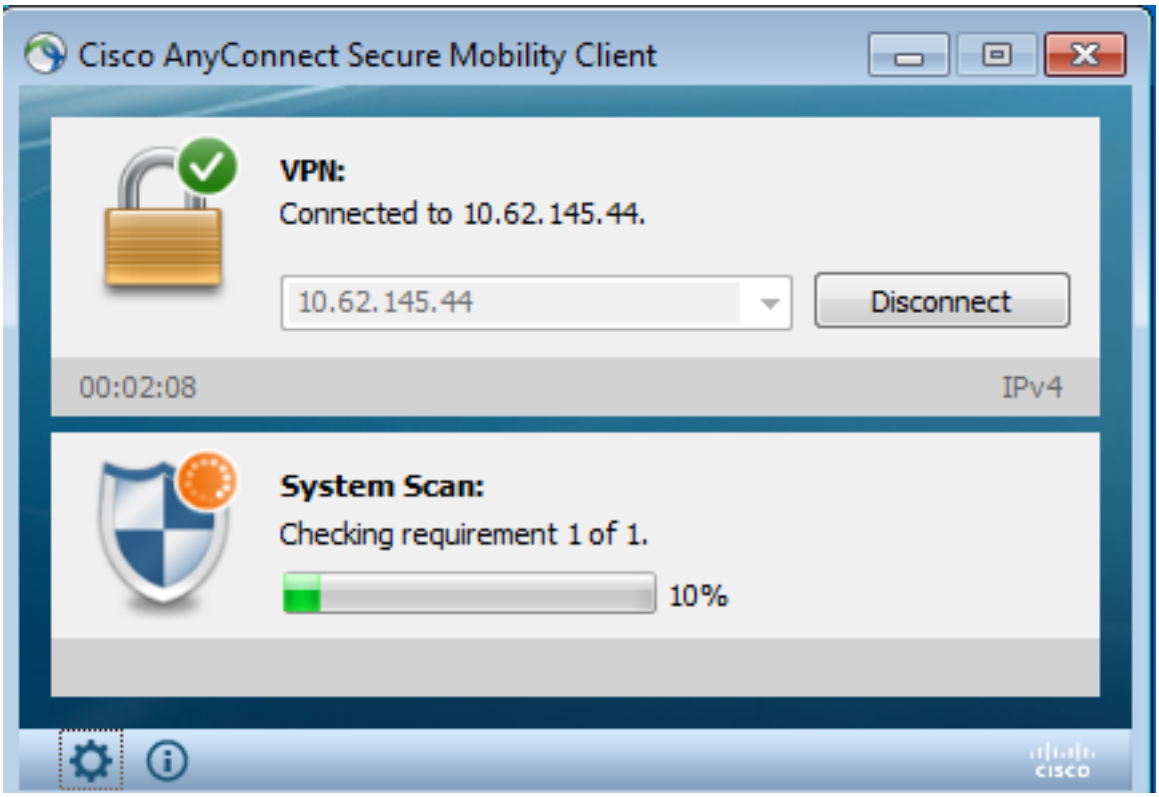


Se necessario, AnyConnect insieme al modulo Posture e conformità viene aggiornato come mostrato nell'immagine.

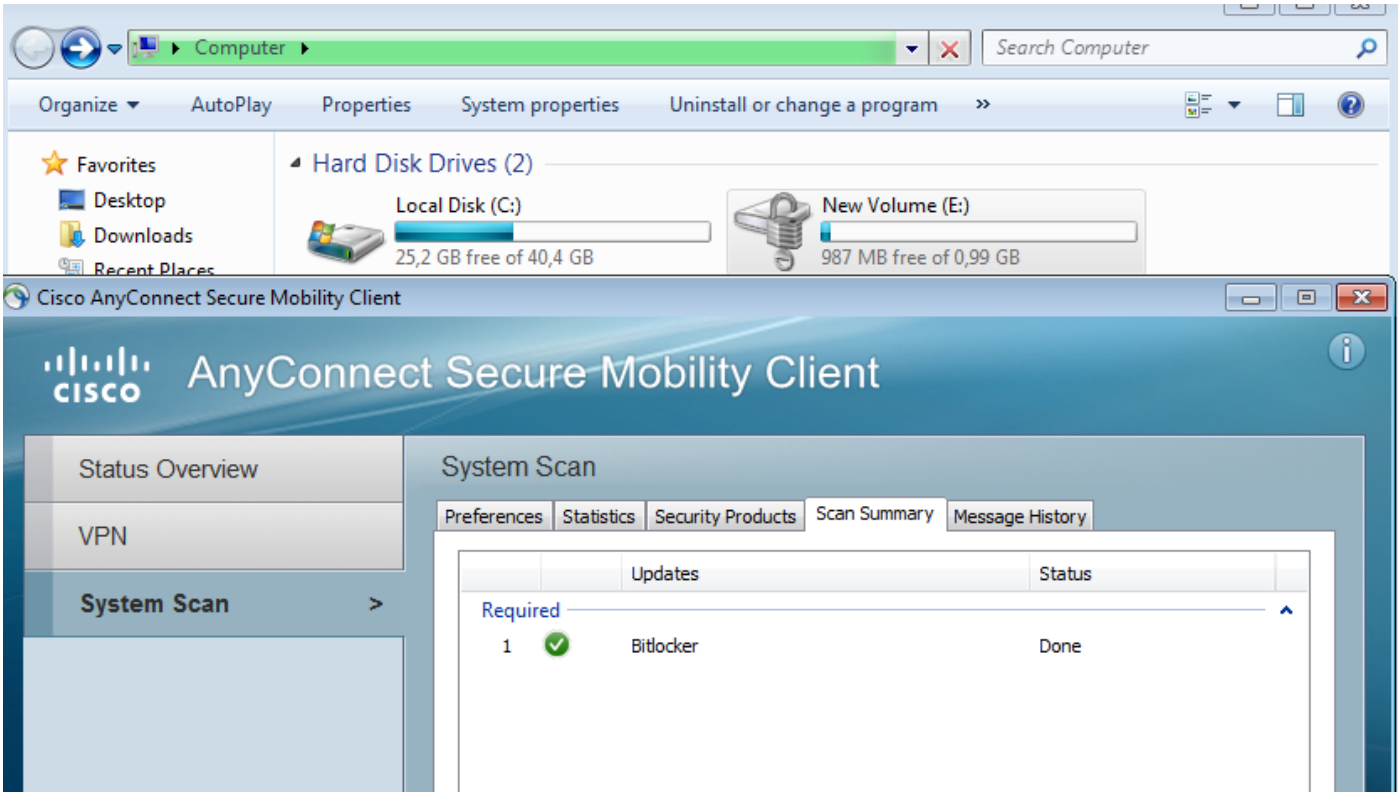


Passaggio 3. Controllo della postura e CoA

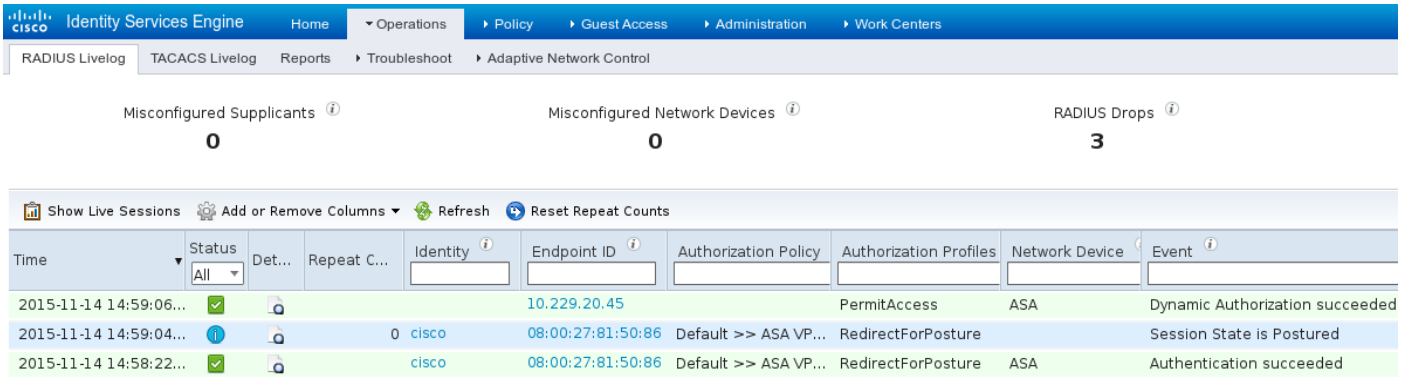
Il modulo Posture viene eseguito, rileva ISE (potrebbe essere necessario avere un record A DNS per enroll.cisco.com per avere successo), scarica e controlla le condizioni di postura come mostrato nell'immagine.



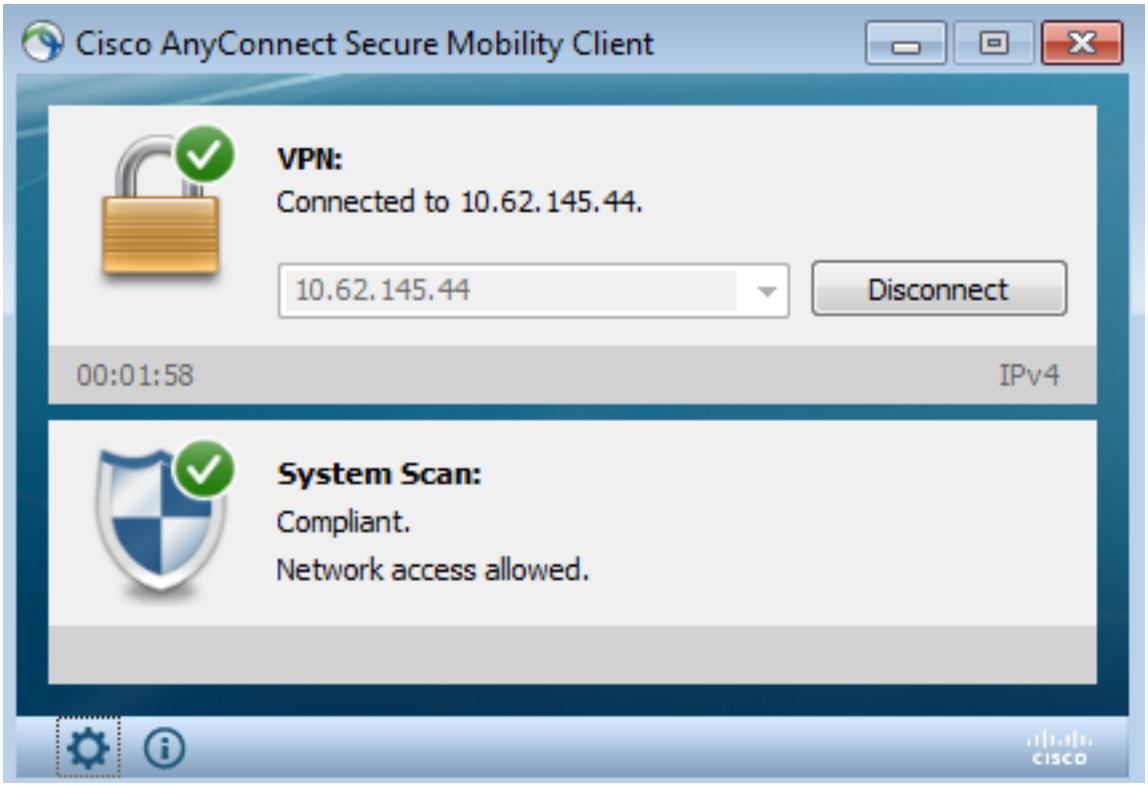
Una volta confermato che **E:** , il report corretto viene inviato ad ISE, come mostrato nell'immagine.



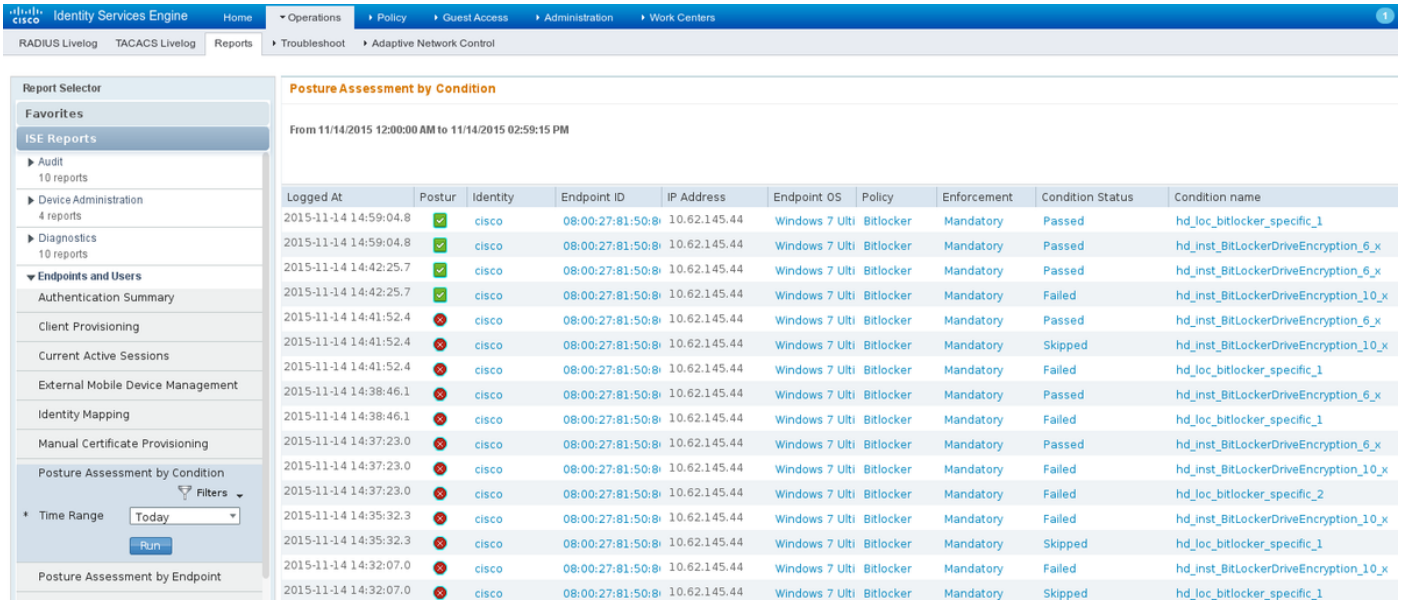
In questo modo il CoA viene attivato per autorizzare nuovamente la sessione VPN, come mostrato nell'immagine.



L'ASA rimuove l'ACL di reindirizzamento che fornisce l'accesso completo. AnyConnect segnala la conformità come mostrato nell'immagine.



Inoltre, rapporti dettagliati sull'ISE possono confermare che entrambe le condizioni sono soddisfatte (**Valutazione della postura per condizione** è il nuovo rapporto ISE 2.0 che mostra ogni condizione). La prima condizione (**hd_inst_BitLockerDriveEncryption_6_x**) controlla l'installazione o il processo, la seconda (**hd_loc_bitlocker_specific_1**) controlla se il percorso specifico (E:) è completamente crittografato, come mostrato nell'immagine.



Il report ISE **Posture Assessment by Endpoint** conferma che tutte le condizioni sono soddisfatte, come mostrato nell'immagine.

Posture More Detail Assessment

Time Range: From 11/14/2015 12:00:00 AM to 11/14/2015 11:42:08 PM
Generated At: 2015-11-14 23:42:08.257

Client Details

Username:	cisco
Mac Address:	08:00:27:81:50:86
IP address:	10.62.145.44
Session ID:	c0a801010001700056473ebe
Client Operating System:	Windows 7 Ultimate 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.2.00096
PRA Enforcement:	0
CoA:	Received a posture report from an endpoint
PRA Grace Time:	0
PRA Interval:	0
PRA Action:	N/A
User Agreement Status:	NotEnabled
System Name:	ADMIN-KOMPUTER
System Domain:	n/a
System User:	admin
User Domain:	admin-Komputer
AV Installed:	
AS Installed:	Windows Defender;6.1.7600.16385;1.141.3676.0;01/11/2013;

Posture Report

Posture Status:	Compliant
Logged At:	2015-11-14 14:59:04.827

Lo stesso può essere confermato dai debug di ise-psc.log. Richiesta di postura ricevuta da ISE e la risposta:

```
2015-11-14 14:59:01,963 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::c0a801010001700056473ebe:::- Received posture
request [parameters: reqtype=validate, userip=10.62.145.44, clientmac=08-00-27-81-50-86,
os=WINDOWS, osVerison=1.2.1.6.1.1, architecture=9, provider=Device Filter, state=, ops=1,
avpid=, avvname=Microsoft Corp.:!::!::!:, avpname=Windows Defender:!::!::!:,
avpversion=6.1.7600.16385:!::!::!:, avpfeature=AS:!::!::!:, userAgent=Mozilla/4.0 (compatible;
WINDOWS; 1.2.1.6.1.1; AnyConnect Posture Agent v.4.2.00096), session_id=c0a801010001700056473ebe
2015-11-14 14:59:01,963 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Creating a new
session info for mac 08-00-27-81-50-86
2015-11-14 14:59:01,963 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Turning on
enryption for endpoint with mac 08-00-27-81-50-86 and os WINDOWS, osVersion=1.2.1.6.1.1
```

```
2015-11-14 14:59:01,974 DEBUG  [portal-http-service28][]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco:c0a801010001700056473ebe:::- Agent criteria
for rule [Name=bitlocker, Description=, Operating Systems=[Windows All],
Vendor=com.cisco.cpm.posture.edf.AVASVendor@96b084e, Check Type=Installation, Allow older def
date=0, Days Allowed=Undefined, Product Name=[com.cisco.cpm.posture.edf.AVASProduct@44870fea]] -
  (  ( (hd_inst_BitLockerDriveEncryption_6_x) )  & (hd_loc_bitlocker_specific_1) )
```

La risposta con il requisito di postura (condizione + correzione) è in formato XML:

```
2015-11-14 14:59:02,052 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
 <version>2</version>
 <encryption>0</encryption>
 <package>
   <id>10</id>




   <version/>




    <type>3</type>
   <optional>0</optional>
   <action>3</action>
   <check>
     <id>hd_loc_bitlocker_specific_1</id>
     <category>10</category>
     <type>1002</type>
     <param>180</param>









     <value_type>2</value_type>
   </check>
   <check>




     <category>10</category>
     <type>1001</type>
     <param>180</param>
```

```
     <operation>regex match</operation>
     <value>^6\..+$|^6$</value>
     <value_type>3</value_type>
   </check>
   <criteria>( (  ( (hd_inst_BitLockerDriveEncryption_6_x) )  &amp;amp;
(hd_loc_bitlocker_specific_1) ) )</criteria>
 </package>
</cleanmachines>
```

Dopo la ricezione del report crittografato da parte di ISE:

```
2015-11-14 14:59:04,816 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Decrypting
report
2015-11-14 14:59:04,817 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Decrypted
report [[
<report><version>1000</version><encryption>0</encryption><key></key><os_type>WINDOWS</os_type><o
sversion>1.2.1.6.1.1</osversion><build_number>7600</build_number><architecture>9</architecture><
user_name>[device-filter-AC]</user_name><agent>x.y.z.d-todo</agent><sys_name>ADMIN-
KOMPUTER</sys_name><sys_user>admin</sys_user><sys_domain>n/a</sys_domain><sys_user_domain>admin-
Komputer</sys_user_domain><av><av_vendor_name>Microsoft
Corp.</av_vendor_name><av_prod_name>Windows
Defender</av_prod_name><av_prod_version>6.1.7600.16385</av_prod_version><av_def_version>1.141.36
76.0</av_def_version><av_def_date>01/11/2013</av_def_date><av_prod_features>AS</av_prod_features
></av><package><id>10</id><status>1</status><check><chk_id>hd_loc_bitlocker_specific_1</chk_id>
```

```
</check><check><chk_id>hd_inst_BitLockerDriveEncryption_6_x</chk_id><chk_status>1></check></pack
age></report> ]]
```

La stazione è contrassegnata come conforme e ISE invia CoA:

```
2015-11-14 14:59:04,823 INFO   [portal-http-service28][]
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a801010001700056473ebe:::- Posture state is
compliant for endpoint with mac 08-00-27-81-50-86
2015-11-14 14:59:06,825 DEBUG  [pool-5399-thread-1][] cisco.cpm.posture.runtime.PostureCoA -
:cisco:c0a801010000f0005647358b:::- Posture CoA is triggered for endpoint [08-00-27-81-50-86]
with session [c0a801010001700056473ebe
```

Inoltre, la configurazione finale viene inviata da ISE:

```
2015-11-14 14:59:04,827 DEBUG  [portal-http-service28][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe:::- Sending
response to endpoint 08-00-27-81-50-86 http response [[ <!--X-Perfigo-DM-Error=0--><!--error=0--
><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--><!--X-Perfigo-Auto-Close-Login-
Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--><!--user role=--><!--X-Perfigo-OrigRole=--
><!--X-Perfigo-UserKey=dummykey--><!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-
Perfigo-Session=--><!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter--><!--X-
Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4--><!--X-Perfigo-DHCP-Renew-Delay=1--
><!--X-Perfigo-Client-MAC=08:00:27:81:50:86--> ]]
```

Questi passaggi possono essere confermati anche dal client (AnyConnect DART):

```
Date         : 11/14/2015
Time         : 14:58:41
Type         : Warning
Source       : acvpnui

Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344
No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[Scanning system ... ]
```

```
****************************************

Date         : 11/14/2015
Time         : 14:58:43
Type         : Warning
Source       : acvpnui

Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344
No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[Checking requirement 1 of 1. ]

****************************************

Date         : 11/14/2015
Time         : 14:58:46
Type         : Warning
Source       : acvpnui

Description : Function: CNacApiShim::PostureNotification
File: .\NacShim.cpp
Line: 461
Clearing Posture List.
```

Per una sessione corretta, usare il comando AnyConnect UI System Scan / Message History per visualizzare la cronologia:

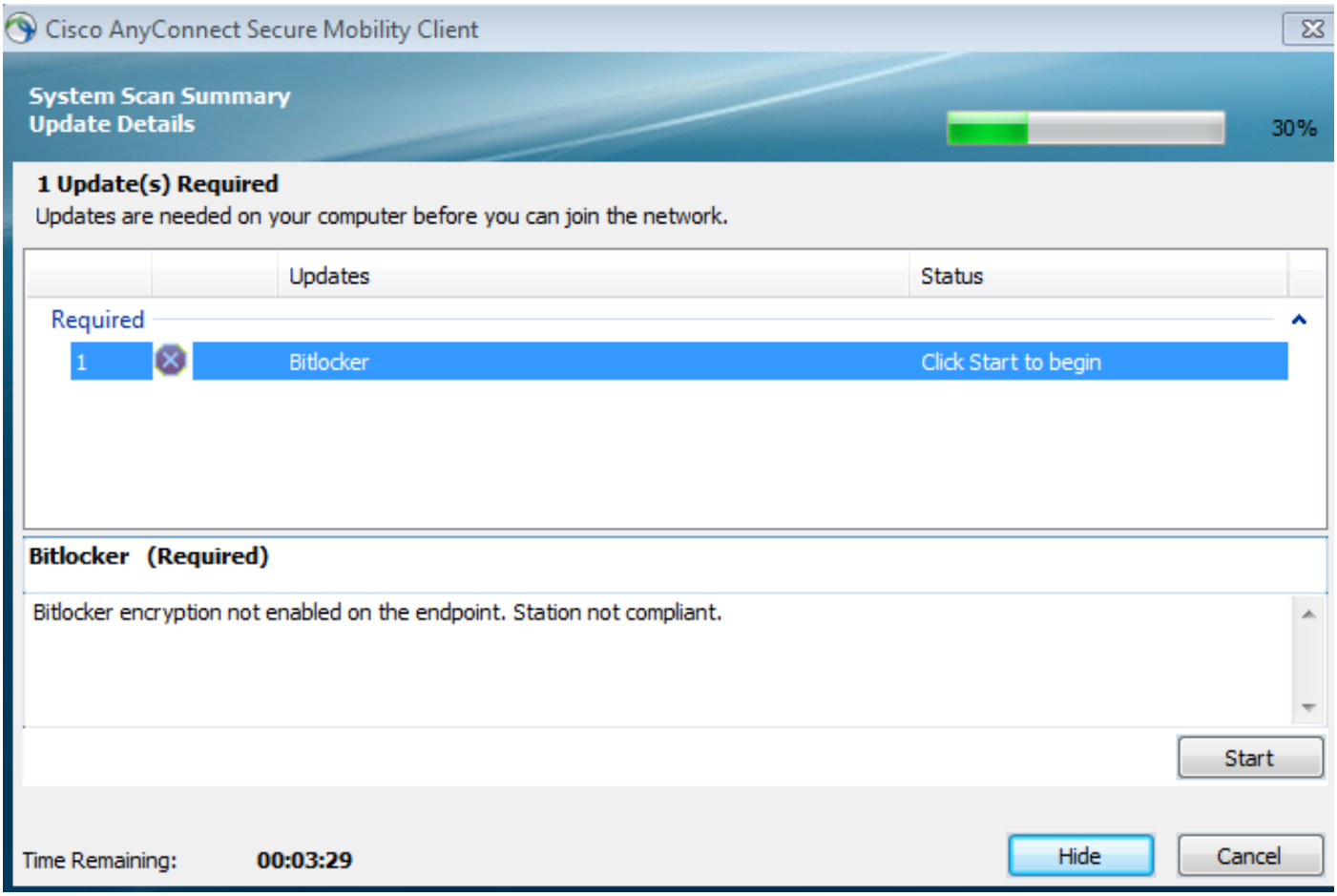
```
     14:41:59    Searching for policy server.
    14:42:03    Checking for product updates...
    14:42:03    The AnyConnect Downloader is performing update checks...
    14:42:04    Checking for profile updates...
    14:42:04    Checking for product updates...
    14:42:04    Checking for customization updates...
    14:42:04    Performing any required updates...
    14:42:04    The AnyConnect Downloader updates have been completed.
    14:42:03    Update complete.
    14:42:03    Scanning system ...
    14:42:05    Checking requirement 1 of 1.
    14:42:05    Updating network settings.
    14:42:10    Compliant.
```

Bug

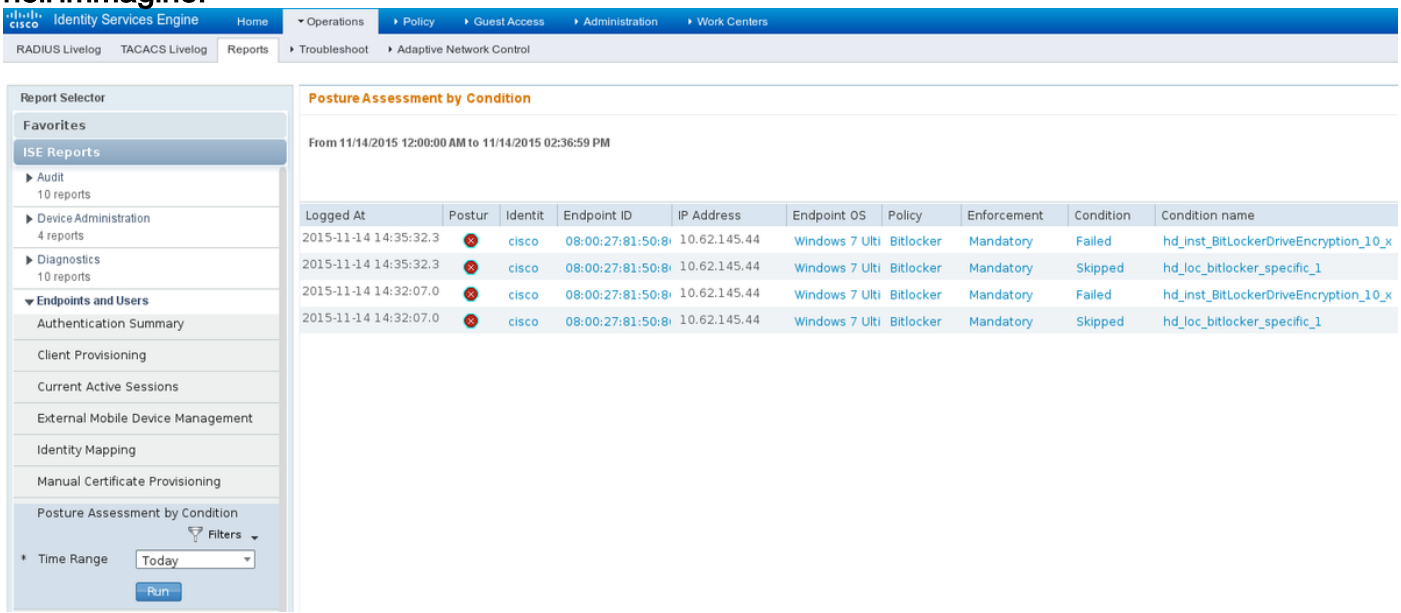
CSCux 15941 - Crittografia bitlocker di postura ISE 2.0 e AC4.2 con errore di posizione (char \ / non supportato)

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.Se l'endpoint non è conforme, viene segnalato dall'interfaccia utente di AnyConnect (viene eseguito anche il monitoraggio e l'aggiornamento configurati) come mostrato nell'immagine.



ISE è in grado di fornire i dettagli sulle condizioni di errore, come mostrato nell'immagine.



Lo stesso può essere verificato dai log CLI (esempi dei log nella sezione Verifica).

Informazioni correlate

- Configurazione di un server esterno per l'autorizzazione utente di Security Appliance
- Guida alla configurazione di Cisco ASA VPN CLI, 9.1
- Guida dell'amministratore di Cisco Identity Services Engine, versione 2.0
- Documentazione e supporto tecnico – Cisco Systems